Attachment 1 68HERD20F0022

**Information Systems Infrastructure Operations,
Software Maintenance & Development,
and Website Management at the Office of Pesticide Programs**

Performance Work Statement

I. Title of Project: Information Systems Infrastructure Operations, Software Maintenance & Development, and Website Management at the Office of Pesticide Programs.

II. Period of Performance: The period of performance of this anticipated award is 12 months, 12/01/2019 thru 11/30/2020.

III. Background

The Environmental Protection Agency (EPA) is responsible for protecting human health and the environment for the United States. The Office of Pesticide Programs (OPP) serves an important role in helping the Agency meet this mandate. In conjunction with other EPA offices, OPP is responsible for the regulation of pesticide production, importation, distribution, and use in the United States.

In 2003, OPP migrated all of its major data systems including regulatory information, scientific data, and workflow tracking into one integrated system, the Office of Pesticide Programs Information Network (OPPIN). OPPIN consolidated information previously stored on the EPA mainframe, the OPP LAN, on stand- alone computers and in paper copy. The purpose of this system was to decrease OPP's data entry burden, increase its analytical capabilities, keep better track of decision-making processes, prevent data loss, improve access to critical decision documents, and make OPP information readily available both within EPA and to stakeholders outside of EPA. As a result of missing functionality, deficiencies in the existing software, data integrity issues, and a variety of other issues, OPPIN was retired in September 2009 and replaced with a new information system named PRISM; the Pesticide Registration Improvement System. PRISM is intended to close existing gaps relating to the EPA mission, replace the current functionalities of the OPPIN system with more efficient tools, create new applications and integrate other existing systems to support data exchange with national and international users and provide current users with a more stable system using newer technologies to enable OPP to continue to meet its' goals and timeframes for pesticides registrations.

To implement this vision of PRISM, existing applications built with older software need to be modernized, outdated processes need to be reexamined, and new technological platforms should be implemented for this effort to be successful. The following will provide background on existing applications to be modernized, new applications to be built, processes to be improved, and new technologies to be implemented.

Several Branches within the Information Technology and Resource Management Division (ITRMD) will participate at the Objective level in the management and oversight of

this Performance Work Statement as technical leads. The Customer Service & Infrastructure Branch (CSIB) is responsible for all servers, hardware, network connectivity, software installation and implementation, operating systems, and other assorted software platforms (Oracle, Lotus Notes, Documentum, etc.). The Systems Design and Development Branch (SDDB) is responsible for the maintenance of existing software and the development of new software for the Office of Pesticide Programs. The Internet and Training Branch (ITB) is responsible for developing, operating, and maintaining software and content of the Pesticides internet websites including OPP's intranet site, OPP@Work. Each of these Branches will provide technical lead for the management of contractor support as described in section **V. Statement of Objectives** of this Performance Work Statement (below).

IV. Scope of Work

The purpose of this contract is to identify and obtain contractor consulting assistance to provide technical, maintenance and operational support, new software development, web development and maintenance of all software including sub-systems for all software applications and other system platform issues. The contractor shall provide such support for all project-related issues associated with all OPP information systems residing on Windows servers, Linux servers, VMware servers, the OPP SAN, the Oracle Real Application Cluster, and all other platforms as required that are currently written for Oracle, Java/J2EE, Documentum, Business Objects, Cold Fusion, Dreamweaver, Adobe, Macromedia, and other application development platforms, as necessary. Support is needed to ensure that OPPIN/PRISM information systems remain readily available to OPP personnel via the LAN and OPP external customers via the Intranet/Internet and other mechanisms (Citrix, remote access via RSA tokens, File Transfer Protocol (FTP) sites, for example). The contractor also shall provide rapid turnaround of enhancements to OPPIN/PRISM. The contractor shall provide maintenance support to correct identified software and data errors and potential enhancements defined as critical to the OPP Mission as well as performing patching and upgrades as required to remediate vulnerabilities and secure the infrastructure. Critical unplanned enhancements may be required as a result of changes to laws governing the pesticide industry.

Place of Performance: The contract requires the Contractor support to be located at EPA's headquarters' physical offices of OPP are located at 2777 Crystal Drive, Arlington, VA or will be relocated to William Jefferson Clinton East Building, 1201 Constitution Ave., N.W. Washington, DC 20004 location in early spring where OPP servers are located. OPP will provide the contractors with office space, phone line, computers, and other Government furnished equipment (GFE) as appropriate for daily use.

Type of Order: This anticipated award will be a Time & Materials task order.

The current RDBMS platform is Oracle 11*g* 10*g* R2 in a Real Application Cluster (RAC) environment. OPPIN/PRISM utilizes Oracle 11*g* Application Server on the middle-tier of an N-tier design. OPPIN/PRISM consists of approximately 1,000 tables, stored procedures, functions, and packages running on Red Hat Linux Enterprise Edition (RHEL). OPP's primary storage is a DELL/EMC Storage Area Network

(SAN) that has an 80 terabyte capacity. The SAN may be upgraded soon. Each of OPPIN/PRISM's various instances, include but are not limited to Development, Test, Staging, Regression & Production occupies approximately 20 GB of Oracle table space (for each instance) OPPIN/PRISM storage requirements are expected grow substantially as document images are added (.TFF and .PDF) making the expansion plans for the SAN necessary.

Several applications currently exist to provide Oracle access to the PRISM user community. The OPPIN DataEntry application is a Powerbuilder "Fat" client/server application used to provide create, retrieve, update, and delete capabilities for OPP staff and management. The OPPIN Query application is an Oracle Application Server 11g compilation of PL/SQL packages that generate HTML source code to provide an internet browser application to retrieve Read-Only collections of OPPIN/PRISM data. Newer applications focus on software developed in Java, at present our environment consist of the following: (subject to change).

COTS Products

Business Objects 4.2 SP04 P08
Documentum 16.4 P06
Apex 5
Power Builder 2017
Kofax 10

Application Servers

Apache Tomcat 7.0.70, 8.5.27
Oracle Weblogic 12c R2/12.2.1 and 12c R1/12.1.3
Jboss/Wildfly 11.0.0
NGINX 1.12.2
Jira 7.11.1

Development Platforms and Frameworks

Java JDK versions vary
Struts 2
Springs versions vary
Flex 3.3, 4
Hibernate versions vary
Tapestry 4
GWT 2.0.4
AngularJS 1.6.x
Ruby on Rails 4.2.6

Hardware

Vendor	**Models**
Cisco	UCS Blades B200M
Cisco UCS Switches	(2)6248 UP
Cisco Network Switches	(2)3830 XS 10G SFG/ (1)3830 XS
Oracle	ODA X-4 L, ODA X-6 HA
NETAPP	FAS8200 Filer – cDOT 9.4(P10)

Operating Systems

Oracle Linux 6.x and 7.x
Red Hat Enterprise Linux 5.x, 6.x, 7.x (x64)
Ubuntu 16.04, 18.04

Windows 2008 R2(x64), Windows 2012 R2 (x64), Windows 2016 (x64)
VMware vSphere 6.7 (x64)

Databases

Oracle 12.1.0.2.0
PostgresSQL 9.6.8
MS SQL versions vary

Infrastructure Applications

NETAPP SNAPMIRROR/SNAPVAULT and McAfee Endpoint Protection

A secondary platform for OPPIN/PRISM is Lotus Notes 8.5.3. ITRMD is currently underway in the process of reassessing all Lotus Notes software included in the OPPIN/PRISM model with plans to redevelop that software using other platforms. Currently, however, Oracle and Lotus Notes interact with each other in OPPIN/PRISM via the Lotus Enterprise Integrator (LEI) 8.5.3. Lotus Notes is used in OPPIN/PRISM to house the OPPTS Directory, a user identification repository, and to hold an assortment of Lotus Notes documents useful to assorted organizations within OPP. Additions, deletions and/or edits made to the OPPTS Directory currently are swept by LEI out of the Lotus Notes documents into temporary Oracle tables every three to five minutes. LEI also is used to update Lotus Notes documents with OPPIN/PRISM data on regular, though less frequent, intervals via a similar mechanism. The future plans are to replace the OPPTS Directory with a new, integrated application using LDAP Server technologies contained in EPA's version of Microsoft Active Directory and may include Oracle Internet Directory (OID) services.

PRISM's discrete data elements are stored in Oracle as attributes of tables. The major collections of metadata within OPPIN/PRISM include:

- Registrations (pesticide products, tolerances, re-registrations, petitions, confidential statements of formula, labels, Jackets, etc.)
- Ingredients
- Companies
- Citations (Study Bibliographies)
- Decision tracking
- Data Call-in (DCI) tracking

Major web browser based Java applications currently in Production include:

- iPRISM
  o Endocrine Disruptor Screening Program (EDSP)
  o Registration Review
- Electronic Submissions (eSubmission)
- Endangered Species
- Section Seven Tracking System (SSTS)
- Label Use Information System (LUIS)
- eCSF (Confidential Statement of Formula)
- eDossier – a stand-alone, non-network application

- Incidents (in development)
- Public Health Tracking System (in development)
- Archive Record Series – a Lotus Notes conversion to Documentum (in development)

OPP also utilizes other system platforms, including:

- Enterprise Content Management System (Documentum)
- Reports using Business Objects

OPP receives a variety of paperwork from industry members wishing to register their pesticide products. The Office also generates a wide array of internal documents, including many for publishing to the registrant community. This makes OPP a very document-rich environment. Currently, the electronic documents can be found in many scattered locations, including network share drives, Lotus Notes repositories, and personal hard drives. The paper documents can be found in many different locations as well, from a controlled file room to individuals' workstations. The decentralized nature of these storage practices makes document retrieval and information sharing difficult, while simultaneously promoting document duplication, versioning issues, and process inefficiencies. OPP has selected EMC²'s Documentum software suite to meet its Enterprise Content Management System needs. A proof-of-concept system was created in 2006 that included the core Documentum functionality, including a baseline Documentum Object Model (DOM). The DOM was then customized to fit the specific needs of OPP, and core search functionality was augmented to fit the new document type and attributes. Three external collections of OPP documents were imported into the repository in order to provide the end user community with a familiar reference point for becoming familiar with the system. The proof-of-concept system was operational in January 2007. The most critical functionality of this
system was solidified soon thereafter, along with several additional modifications. By June 2007, a production system was rolled out that included a collection of Studies received by OPP (one of the three initial collections of data). In January 2010, OPP upgraded its Documentum repository from v5.3 to v6.5. However, the Web Services of the eSubmission application needs to be rebuilt as it was designed in a framework not supported by v6.5.

Business Objects provides comprehensive business intelligence solutions and functionality via access to canned and ad-hoc OPPIN/PRISM reports. Two servers are used within the OPPIN environment in support of the Business Objects functionality, including a Business Objects XI R2 server (Apache 2.0.46 / Tomcat 4.1.27) and database server (Oracle 9.2.0.5). The Business Objects environment will be fully integrated into the current OPPIN architecture and will host the Document, Security, and Universe domains.

Website development, operations and maintenance, and the management of content of the Pesticides internet website are objectives for which a contractor may be responsible. Examples of the type of work a contractor could be responsible for may include:

- Development of new web pages and projects

    - Develop a variety of major projects each year (eg. Pesticide Application Registrations, Pesticide Registration Manual (Blue Book), etc.)
    - Develop hundreds of new pages each year
    - Edit, correct and update thousands of pages each year

- Develop or significantly enhance existing web applications
    - New Search Mechanisms
    - Pesticide Product Label System (PPLS)
    - Incident Portal

- Maintain existing web applications and databases
    - Section 18
    - Food and Feed
    - Pesticide Product Information System (PPIS)
    - Troubleshoot and solve technical problems across all parts of the Pesticides website

- Lead Efforts to Utilize Web 2.0 Tools and Implement the Open Government Initiative
    - Web 2.0 Training and Planning
    - Public Participation
    - Provide OPP resources for Data.Gov and other new sites

- Ensure Compliance with Agency and OPP Web Standards
    - Agency web standards, web guide, etc
    - OPP and OPPTS SOPs
    - Section 508 compliance on all Web products to include PDF documents

- Plan and Manage Transition to Agency's Web CMS Platform
    - Develop OPP Metadata Standard and Implementation Plan
    - Develop Information Architecture
    - Identify and consolidate Web content through ROT (Redundant, Outdated, and Trivial)
    - Represent OPP and OPPTS on transition

- Enhance and Maintain OPP@Work
    - Lead comprehensive redesign effort
    - Implement new pages and features for customers
    - Edit and update daily

- Analyze and Report on Web Usage Statistics
    - Develop Pesticides Website Annual Report
    - Provide custom reports for customers

V. Statement of Objectives

The requirements contained in this contract are considered performance-based, focusing on OPP's desired results and outcomes. The contractor shall be responsible for determining the most effective means by which these requirements will be fulfilled. In order to fulfill the requirements, the contractor shall design innovative processes and systems that can deliver the required services in a manner that will best meet the OPP's Performance Objectives. This performance-based requirement represents a challenge to the contractor to develop and apply innovative and efficient approaches for achieving results and meeting or exceeding the Performance Objectives, measures, and standards described below. OPP will monitor the contractor's performance in accordance with the Quality Assurance Surveillance Plan as described within each Objective.

Under this performance work statement, OPP defines the desired outcome and, in turn, the contractor proposes the most efficient methods to achieve results that fulfill the desired outcome. Typical areas that are measured include cost control, timeliness and completeness of deliverables, problem resolution, business relations, quality of work performed, and whether or not the deliverable assists OPP in meeting its objectives and goals as identified in this Statement of Requirements.

In cases where Performance Objectives and minimum Acceptable Quality Levels (AQLs) are not being met, the contractor will make every effort to immediately correct the problem to ensure customer satisfaction. If the problem is systemic, the contractor will submit a plan of corrective action to the TOCOR.

Please note that for all Performance Objectives, the Contractor Incentive is that for at least three (3) or more written warnings of inadequate deliverable quality throughout the contract performance period, the Contractor will be penalized 10% (ten percent) from the total due per performance objective on the submitted monthly invoice.

Performance Object 1: Project Management (Mandatory)

Sub-Task 1: Project Management

The contractor shall provide a single point of contact for the management of all aspects of the tasks involved with this contract. That person shall be known as the contractor project manager. The contractor project manager shall report on all aspects of the objectives of this contract to the designated OPP Task Order Contract Officer Representative (TOCOR) or designated Alternate (ATOCOR). The contractor project manager shall provide, in writing, all requirements needed by the contractor to accomplish the goals set out in this document. During monthly status meetings, the contractor shall verbally notify the TOCOR of any significant difficulties in accomplishing the agreed upon task list. The contractor shall immediately notify the TOCOR/ATOCOR of any factor or change that may significantly affect the approved schedule.

Transition Period

The Contractor Team shall work with the current contractor staff for a minimum of thirty days for a detailed knowledge transfer. This will include but not be limited to

operations and maintenance of the SCR (system change request) tracking system, operations and management procedures of the infrastructure, operations and management of our development, test and production environments.

Task 1.1 - Project Management

The Contractor Team shall provide a single point of contact for the management of all aspects of the tasks involved with this Performance Work Statement. That person shall be known as the Contractor Project Manager. The Contractor Project Manager shall report on all aspects of the objectives of this contract to the designated OPP Task Order Contract Officer Representative (TOCOR) or designated Alternate (ATOCOR). The Contractor Project Manager shall provide, in writing, all requirements needed by the Contractor to accomplish the goals set out in this Performance Work Statement. The Contractor Project Manager shall verbally notify the TOCOR/ATOCOR of any significant difficulties in accomplishing the task list agreed to at the weekly meeting.

The Project Management Plan (PMP) is a document describing the overall program structure; deliverables; related management plans and procedures; and the methods used to plan, monitor, control, and improve the project development efforts. The PMP is a dynamic document and is expected to be updated on a periodic basis to reflect organizational changes, lessons learned, and advances in methodologies that occur throughout the project's life cycle. The Contractor Program Manager shall provide a Project Management Plan within ten (10) days of contract award.

The Contractor Project Manager shall be responsible for ensuring that the services and deliverables required by the EPA System Life Cycle are provided. At the time a task is identified, the TOCOR/ATOCOR will determine when and if a specific project management plan is required. A Project Management Plan shall be required for complex or long-term tasks requiring extensive analysis, development, testing, or planning and coordination with other resources as determined by the TOCOR/ATOCOR. If a project management plan is required, the Contractor Project Manager shall ensure that the plan is created and presented to the TOCOR/ATOCOR. The Project Management Plan shall identify all tasks, resources, schedule, assumptions, and risks associated with the Performance Objective. The Project Management Plan shall require concurrence by the TOCOR/ATOCOR and shall become the official schedule for the Performance Objective. The Project Management Plan shall be maintained and updated by the Contractor Project Manager to reflect actual accomplishments, delays, or additional tasks identified for the duration of the Performance Objective and shall be provided to the TOCOR/ATOCOR as needed. The Contractor Program Manager shall immediately notify the TOCOR/ATOCOR of any factor or change that may significantly affect the approved schedule.

The Contractor Project Manager shall use the established Configuration Management (CM) tool in use by OPP to collect and store all deliverables. The design descriptions and diagrams stored in the CM tool shall be the foundation for specifications to be used to update PRISM software.

The contractor shall manage the new development projects using an Agile Development methodology; vendors are encouraged to use CMMI Level III best practices, but this is not required. The contractor will generate and deliver a Deliverable Product Acceptance (DPAF) as required to ensure concurrent acceptance of all parties involved to ensure completeness of a deliverable. In addition, the contractor will deliver all system deliverables in a 508 compliant format.

Deliverable & Schedule for Task 1.1

The contractor shall participate in monthly project status meetings, shall deliver biweekly schedule updates, and shall provide biweekly project status updates via email. Biweekly status updates shall describe Work performed, Work status, Work progress difficulties encountered, remedial actions, and statement of Deliverable(s) anticipated subsequent to the reporting period.

Each biweekly status update shall include, but is not limited to, the following sections:

Narrative Summary:
This section shall be a thorough statement of the Project activities and progress during the previous two weeks. It should include a discussion of any problems encounters, and any proposed changes to the work set forth in this PWS.

Scheduled status:
This section shall state whether the project is progressing according to the target deliverable dates set forth in this PWS. If delays have been experienced, the section shall include a discussion of how the project will be brought back on schedule or any necessary revision to the schedule.

Activities planned for next period:
This section shall include a discussion of the work and associated deliverables anticipated in the next period.

Open Issues:
When appropriate, this section shall include a discussion of open issues and methods proposed for issue resolution. This section shall assign specific resources (Contractor or EPA staff) to issues in an effort to obtain timely resolution.

A monthly report, to be submitted within five (5) working days after the close of the contractor invoice cycle shall be submitted. The monthly report must contain the hours of technical support provided, and a summary of the progress toward the completion of all requirements of the contract. This shall include current month data, as well as year-to-date data in both hours/dollars.

Task 1.2 - Task Management Cost Accounting

The Contractor Program Manager shall produce a cost accounting report detailing the Budget, Actual Expenditures, and Variances down to the system level

(Work Breakdown Structure [WBS] Level 3). The Contractor Program Manager shall use standard EPA practices for performing Earned Value Management and other generally accepted accounting practices.

The contractor shall prepare a Monthly Progress Report for distribution to the TOCOR. This report (which includes the Monthly Financial Report) will contain information regarding the routine and ad hoc activities performed, along with the funds and labor hours expended, under the Contract(s). The contractor will monitor the performance objectives for this contract that are detailed in the Quality Assurance Surveillance Plan. The contractor will make every effort to immediately inform USEPA of any significant difficulties encountered during the period of performance of this work.

The Contractor shall provide monthly Earned Value Management (EVM) reports for its deliverables and costs by the tenth (10^{th}) business day following the end of the month. This report shall detail the EVM data separately for each of the contracts defined. In addition, the Contractor shall have the capability, at the TOCORs/ATOCORs request (for future months), to produce EVM reports which segregate EVM data for any or all tasks between a particular project and other efforts during a month. The Contractor shall use standard EPA practices for performing EVM and other generally accepted accounting practices. The Contractor shall provide an analysis and explanation of any significant variances, positive or negative, in the EVM measures with suggestions for remediation where appropriate. The Contractor shall also reconcile any discrepancies between the monthly EVM data and the invoice. The contractor will notify, in writing, the USEPA Project Officer (PO), CO, and TOCOR when 75% of the labor hours for work under any of the Contracts have been expended.

Task 1.3 Acquisition of Signature of Approval

The concurrent acceptance of work deliverables is based on the acquisition of signatures of specified stakeholders and/or members of workgroups assigned to the Project as identified in each Project's Charter. Currently, a signed electronic Deliverable Product Acceptance Form (eDPAF) represents the concurrent acceptance of all parties involved of the completion of a task's deliverable satisfying an Objective of this Performance Work Statement (PWS). The eDPAF is required at every stage of the SDLC process and/or for each deliverable for each task of this PWS. The Contractor shall work with the TOCOR/ATOCOR to ensure a fully-signed eDPAF is completed as required by each identified task of this PWS. See Appendix 1 for an example of an eDPAF. The list of signatures required by the eDPAF will be determined by the TOCOR/ATOCOR based on the nature of the specific Objective. . The Contractor shall ensure a PDF version of the signed eDPAF is saved into EPA OPPIN Software Configuration Management Tool (VM-OPPIN).

Task 1.4 Version Control and Configuration Management

The Contractor shall use the OPP Configuration Management tool (presently Apache Subversion but subject to change as determined by the TOCOR/ATOCOR) to

VM-OPPIN) (http://dcoppscm01.cmii.epa.gov/) to collect and store final functional requirements document, final design document, final prototype code, software source code, meeting minutes, agendas, summaries, and all other documentation and notes gathered at or for the Workgroup sessions described in this Performance Work Statement.

Documentation stored in the Configuration management System shall be the foundation for specifications to be used to update PRISM software to incorporate Incidents information. The TOCOR/ATOCOR will provide specific requirements of version control to the Contractor after award.

Performance Objective 1: Program Management

Quality Assurance Surveillance Plan

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE
Performance Objective 1: Project Management				
1) Submit high quality deliverables to TOCOR/ATOCOR in a timely manner.	1) All document deliverables are clear, well organized, and free of typographical, spelling, and formatting errors.	1) Documents are delivered on time; no more than five (5) typographical, spelling, and formatting errors identified in any draft or final document.	1) The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved.	Please see page 7.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE
Performance Objective 1: Project Management				
2) Perform and task-level program management	2) Weekly status meetings are held; agendas, meeting minutes, and updated project management plan are provided. Work Breakdown Structures are provided for Objectives and Tasks.	2) Up-to-date project management plan is provided at 95% of status meetings. Status reports contain prioritized Performance Objective lists and accurate lists of accomplishments 95% of the time. Work Breakdown Structures are provided for 95% of all Objectives and Tasks as determined by the TOCOR/ATOCOR.	2) The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved.	Please see page 7.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE
Performance Objective 1: Project Management				
3) Collect and store documentation in CM tool.	3) All deliverables and documents relevant to this objective (including notes, agendas, etc.) are to be stored in Version Manager tool.	3) 95% (ninety-five percent) of deliverables and documents are stored in Version Manager tool.	3) The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved.	Please see page 7.

NOTE: Performance Objectives 2 through 27 will be managed exclusively by the Customer Service & Infrastructure Branch (CSIB) of the Information Technology & Resource Management Division (ITRMD). CSIB will provide Subject Matter Experts Technical Point of Contacts for each Performance Objective according to the needs of Branch management and staff. A Quality Assurance Surveillance Plan (QASP), appears at the end of Performance Objective 27. This QASP should be considered appropriate for all Infrastructure Management and Production System Administration identified within these Objectives.

Performance Objective 2: Storage Area Network (SAN)

Administration (Mandatory) <u>Subtask A: Storage Area Network</u>

<u>(SAN) Management</u>

The Contractor shall in conjunction with CSIB be responsible for the management and administration of the SAN, including management of RAID groups, logical units (LUNs), server attachment to the SAN including installation of Powerpath and Navisphere client software, and allocation and activation of SAN-attached storage on the servers. The Contractor will document changes made to the SAN layout and periodically provide reports, charts etc. to EPA detailing the configuration and space allocation. Duties may also include providing NETAPP management to provide cloning, snapshot and DR services as well as other NETAPP services as required.

Subtask B: Fibre Channel (FC)and/or iSCSI Network Management

Contractor shall in conjunction with CSIB be responsible for the management of the fibre channel and/or iSCSI network including the FC switches used to provide connectivity between the SAN storage unit, attached servers, and tape library. Duties would include zone management to provide connectivity between the server and SAN hosted storage.

Subtask C: SAN/FC and or NETAPP and iSCSI Network Maintenance

The Contractor shall in conjunction with CSIB be responsible for day to day monitoring of the health of the SAN and FC network, notifying EPA of problems, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying client product patches and upgrades to the product as recommended by the EPA or the vendor.

Performance Objective 3: VMware

Administration (Mandatory) Subtask

A: VMware Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of the VMware server environment. Duties include installation and configuration of VMware ESXi or Vsphere on servers in accordance with EPA SCDs and other guidance documents, the allocation of SAN attached storage to VMware, allocation of virtual machines containing RedHat Linux or Windows servers, and implementation of VMware features such as Virtual Motion, Dynamic Resource Scheduling, Disaster Recovery, and Backup.

Subtask B: VMware Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the VMware environment using VM Virtual Center, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor.

Performance Objective 4: Windows Server Administration (Mandatory)

Subtask A: Windows Server Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's physical and virtual Windows servers in the development, test and production environments. Duties include installation of Windows server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), setting up the operating system environment to host EPA standard software.

Subtask B: Windows Server Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Windows servers, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the operating system as recommended by the EPA or the vendor, and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Subtask C: Windows Active Directory Maintenance

Contractor shall in conjunction with CSIB be responsible adding and removing EPA AD user, server, and group accounts from various OPP-controlled AD groups. AD certification is required to perform this duty.

Performance Objective 5: RedHat Linux Server

Administration (Mandatory) Subtask A: Redhat

Linux Server Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's physical and virtual Redhat Linux servers in the development, test and production environments. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), setting up the operating system environment to host EPA standard software. Expertise is explicitly required for the support of Oracle's Real Application Cluster (RAC) software and database on Linux.

Subtask B: Redhat Linux Server Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Linux servers, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 6: Production Oracle Database/Real Application Cluster (RAC) Administration (Mandatory)

Subtask A: Production Oracle Database/RAC Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Oracle databases and Real Application Clusters (RAC). Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying Oracle databases, managing users, security, storage, schemas, performance, and database backup and recovery.

Subtask B: Oracle Database/RAC Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Oracle Database/RAC Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Oracle databases/clusters, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 7: Production Microsoft SQL Server

Administration (Mandatory) Subtask A: Production Microsoft

SQL Server Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production SQL server databases. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying SQL server databases, managing users, security, storage, schemas, performance, and database backup and recovery.

Subtask B: Microsoft SQL Server Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: ContractorMicrosoft SQL Server Maintenance

The contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Oracle databases/clusters, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor, and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 8: Production Oracle Internet Application Server

Administration (Mandatory) Subtask A: Oracle Internet Application Server (iAS) Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Oracle Internet Application Server environment. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying managing Oracle iAS applications.

Subtask B: Oracle Internet Application Server (iAS) Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Oracle Internet Application Server (iAS) Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Oracle internet application server environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 9: Production Microsoft SharePoint

Administration (Optional) Subtask A: SharePoint Application Server Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Microsoft SharePoint Server environment. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying managing Microsoft SharePoint applications.

Subtask B: Microsoft SharePoint Change Management

The Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Microsoft SharePoint Server Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to

day monitoring of the health of the production Microsoft SharePoint Server environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 10: Citrix Server/Farm

Administration (Mandatory) Subtask A: Citrix

Server/Farm Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's Citrix Metaframe Presentation Server environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing the software, components, adding/removing applications, security and performance.

Subtask B: Citrix Server/Farm Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Citrix Server/Farm environment, working with the vendor to obtain technical support and to implement solutions to problems malfunctions.

Performance Objective 11: Microsoft Remote Desktop Services

Administration (Optional) Subtask A: Microsoft Remote

Desktop Services Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's Microsoft Remote Desktop Services Server environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing the software, components, adding/removing applications, security and performance.

Subtask B: Microsoft Remote Desktop Services Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Microsoft Remote Desktop Services environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 12: Production Documentum

Administration (Mandatory) Subtask A: Documentum

Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Documentum environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying Documentum-related applications and services.

Subtask B: Documentum Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Documentum Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Documentum environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 13: Production Kofax

Administration (Mandatory) Subtask A: Kofax

Management

Contractor shall in conjunction with SDDB/CSIB be responsible for the management and administration of OPP's production Kofax environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying Kofax related Batch Class applications, components, Kofax Server/Client Software upgrades and services.

Subtask B: Kofax Change Management

Contractor shall in conjunction with SDDB/CSIB be responsible for implementing changes to the production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Kofax Maintenance

Contractor shall in conjunction with SDDB/CSIB be responsible for the day to day monitoring of the health of the production Kofax environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with SDDB/CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 14: Production Lotus Domino Server

Administration (Optional) Subtask A: Lotus Domino Server

Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Lotus Domino server environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing databases, applications and performance.

Subtask B: Lotus Domino Server Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions received from the development team in order to upgrade applications and databases from the development/test environment to the production environment.

Subtask C: Lotus Domino Server Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Lotus production Domino server environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor, and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 15: Production Lotus Enterprise Integrator (LEI)

Administration (Optional) Subtask A: Lotus Enterprise Integrator (LEI)

Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Lotus Enterprise Integrator environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing operations and performance of the application.

Subtask B: Lotus Enterprise Integrator (LEI) Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Lotus Enterprise Integrator (LEI) Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Lotus Enterprise Integrator environment, working with the vendor to obtain technical support and to implement solution to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patch and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to prov to EPA for reporting or auditing purposes.

Performance Objective 16: Production Business Objects Administration (Mandatory)

Subtask A: Business Objects Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's production Business Objects environment. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing the operation of the environment.

Subtask B: Business Objects Change Management

The Contractor shall in conjunction with CSIB be responsible for implementing changes to the production environment based on directions received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Business Objects Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the production Business Objects environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 17: EM7

InfraView (Optional)

Subtask A: EM7 InfraView

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's EM7 InfraView monitoring environment for the development, test and production environments. Duties include

configuration of the software Communication environment following EPA's Standard Configuration Documents (SCDs), managing the operation of the environment.

Subtask B: EM7 Infraview Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the EM7 InfraView environment, working with the Infraview Admin group in RTP to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 18: Data Backup/Restore/DR – VEEAM/Backup Exec/Acronis Image Managment (Mandatory)

Subtask A: Backup Exec/VEEAM – Backup/Restore/DR Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's Backup Exec and VEEAM environments for the development, test and production environments. Duties include installation of software, including agents on servers, executing backup jobs, restore jobs, developing/following proper backup schedules and procedures, including the backup of Oracle databases, Documentum repositories, other OPP data as required, media management, transportation to off-site storage, ensuring that OPP data can be recovered in the event of hardware/software failures, synchronization of data with DR site.

Subtask B: Acronis Image Management

Contractor shall in conjunction with CSIB be responsible for using Acronis TrueImage software to maintain an up-to-date inventory of OPP server drive images, the ability to restore images to malfunctioning servers if necessary, transportation of images to off-site storage.

Subtask C: Data Backup/Restore/DR – VEEAM/Backup Exec/Acronis Image Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Backup Exec and VEEAM environments, ensuring jobs run successfully, conducting test restore operations, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendors and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 19: Development/Test and other non-production Oracle Database/Real Application Cluster (RAC) Administration (Optional)

Subtask A: Oracle Database/RAC Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test and other non-production Oracle databases and Real Application Clusters (RAC). Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying Oracle databases, managing users, security, storage, schemas, performance, and database backup and recovery.

Subtask B: Oracle Database/RAC Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions and scripts received from the development team in order to upgrade applications in these environments.

Subtask C: Oracle Database/RAC Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the development and test and other non-production Oracle databases/clusters, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 20: Development/Test and other non-production Microsoft SQL Server Administration (Optional)

Subtask A: Development/Test and other non-production Microsoft SQL Server Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's Development/Test and other non-production SQL server databases. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying SQL server databases, managing users, security, storage, schemas, performance, and database backup and recovery.

Subtask B: Microsoft SQL Server Change Management

The Contractor shall in conjunction with CSIB be responsible for implementing changes to the Development/Test and other non-production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Microsoft SQL Server Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Development/Test and other non-production environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 21: Development/Test and other non-production Oracle Internet Application Server Administration (Optional)

Subtask A: Oracle Internet Application Server (iAS) Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test and other non-production Oracle Internet Application Server environment. Duties include installation of server software, configuration of the software following
EPA's Standard Configuration Documents (SCDs), creating/modifying managing Oracle iAS applications.

Subtask B: Oracle Internet Application Server (iAS) Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions and scripts received from the development team in order to upgrade applications in these environments.

Subtask C: Oracle Internet Application Server (iAS) Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the development and test and other non-production Oracle internet application server environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 22: Development/Test and other non-production Microsoft SharePoint Administration (Optional)

Subtask A: SharePoint Application Server Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's Development/Test and other non-production Microsoft SharePoint Server environment. Duties include installation of server software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying managing Microsoft SharePoint applications.

Subtask B: Microsoft SharePoint Change Management

The Contractor shall in conjunction with CSIB be responsible for implementing changes to the Development/Test and other non-production environment based on directions and scripts received from the development team in order to upgrade applications from the development/test environment to the production environment.

Subtask C: Microsoft SharePoint Server Maintenance

The Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Development/Test and other non-production Microsoft SharePoint server environment, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor, and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 23: Development/Test and other non-production Documentum Administration (Optional)

Subtask A: Documentum Management

The Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test and other non-production Documentum environments. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), creating/modifying Documentum-related applications and services.

Subtask B: Documentum Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions and scripts received from the development team in order to upgrade applications in these environments to the production environments.

Subtask C: Documentum Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the development and test and other non-production Documentum environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 24: Development/Test Kofax Scanning

Software (Optional) Subtask A: Kofax Administration

Management

Contractor shall in conjunction with SDDB be responsible for the development management and administration of OPP's development and test and other non-production Kofax Server/Client environments. Duties include installation of software, configuration of the software development, andsoftware integration following EPA's Standard Configuration Documents (SCDs).

Subtask B: Kofax Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions received from the development team in order to upgrade (Server/Client) applications in these environments.

Subtask C: Kofax Maintenance

Contractor shall in conjunction with SDDB/CSIB be responsible for the day to day monitoring of the health of the Kofax development and test and other non-production Kofax environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions.
The Contractor shall be responsible for applying product patches, software (Server/ Client) modifications, and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 25: Development/Test Lotus and other non-production Domino Server Administration (Optional)

Subtask A: Lotus Domino Server Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test and other non-production Lotus Domino server environments. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing databases, applications and performance.

Subtask B: Lotus Domino Server Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions received from the development team in order to upgrade applications and databases in these environments.

Subtask C: Lotus Domino Server Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the Lotus development and test and other non-production Domino server environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 26: Development/Test Lotus Enterprise Integrator (LEI) Administration (Optional)

Subtask A: Lotus Enterprise Integrator (LEI) Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test Lotus Enterprise Integrator environments. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing operations and performance of the application.

Subtask B: Lotus Enterprise Integrator (LEI) Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test environments based on directions received from the development team in order to upgrade applications in the development and test environments.

Subtask C: Lotus Enterprise Integrator (LEI) Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the development and test Lotus Enterprise Integrator environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor will be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

Performance Objective 27: Development/Test and other non-production Business Objects Administration (Optional)

Subtask A: Business Objects Management

Contractor shall in conjunction with CSIB be responsible for the management and administration of OPP's development and test and other non-production Business Objects environments. Duties include installation of software, configuration of the software following EPA's Standard Configuration Documents (SCDs), managing the operation of the environment.

Subtask B: Business Objects Change Management

Contractor shall in conjunction with CSIB be responsible for implementing changes to the development and test and other non-production environments based on directions received from the development team in order to upgrade applications in the development and test environments.

Subtask C: Business Objects Maintenance

Contractor shall in conjunction with CSIB be responsible for the day to day monitoring of the health of the development and test and other non-production Business Objects environments, working with the vendor to obtain technical support and to implement solutions to problems and malfunctions. The Contractor shall in conjunction with CSIB be responsible for applying product patches and upgrades to the product as recommended by the EPA or the vendor and maintaining a spreadsheet/database to provide to EPA for reporting or auditing purposes.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE (CI)
Infrastructure Management and Production System Administration for Performance Objectives 2-27				
1) System administration is performed correctly, timely and accurately. 2) Production system management is performed correctly, timely and accurately.	1) System administration results in a stable, properly functioning, and up-to-date environment with a minimum of downtime or disruption due to contractor error or inaction. 2) Production system management results in a stable, properly functioning, and up-to-date environment with a minimum of downtime or disruption due to contractor error or inaction.	1) Provide accurate and complete documentation of projects and tasks performed, including charts and diagrams of the infrastructure. 2) Production system is operational 99% (ninety-nine) of the time.	The Contractor shall be alerted, in writing, whenever performance objectives are not achieved.	1) Please see page 7. 2) Please see page 7.

NOTE: Performance Objectives 28 through 30 will be managed exclusively by the Systems Design & Development Branch (SDDB) of the Information Technology & Resource Management Division (ITRMD). SDDB will provide Subject Matter Experts Technical Point of Contacts for each project created for a specific Performance Objective according to the needs of Branch management and staff. Quality Assurance Surveillance Plans (QASP) appear after each Performance Objective and are appropriate only for projects associated with that specific Objective.

Software Maintenance Objectives

EPA/OPP's software development cycle is managed in two very distinct phases; the initial development (which also includes major upgrades) cycle and the operations and maintenance cycle. This comes with several challenges:

- Knowledge transfer: The personnel working on the legacy code must diligently document the code and all edits with dates and personnel identification in order to fill in gaps from documentation or to understand certain procedures that exist.
- Test coverage: Test scripts and/or data used during original development are not available to the maintenance team.
- Code baselines: The version of source code provided to the development team during a major upgrade isn't worked on (except for issues that warrant an Emergency release) while it is undergoing that major revision. Passing these patches to the development team requires validation that they have been incorporated or merging of the branch to the trunk by the maintenance contractor team.

Issue prioritization is also categorized based on the severity of the issue and business priority. Critical severity issues are those that cause malfunction of the system or are corrupting data within the system, rendering the system unreliable; these are automatically High business priority. Major severity issues are those where a function cannot be performed as intended within the system and no reasonable work-around exists for performing that function; Moderate severity is where reasonable work-arounds exist or the functions need minor changes; and Minor severity is for changes that are cosmetic in nature. High business priority issues are those critical to the work OPP performs; Medium priority is for issues that assist the business in their function, but are not required by statute, regulation, policy, or other key requirement; Low business priority issues are those that are optional.

Most software maintenance work is conducted as a continuous stream of tasks with code changes branched from the trunk of the main release and then merged back into the trunk after being tested and tagged for production release. Some software maintenance work, usually that which is more significant in nature, but not enough for becoming its own task, is conducted as a project, with pre-defined start and end points. These are managed in short weekly iterations until the product (application code) is ready for release.

Currently all issues (as System Change Requests, SCRs) are tracked within our issue tracking system: Source code management is maintained in Subversion.

Required Skills

Applications are a mix of custom client/server, stand-alone/non-networked applications, Commercial Off-The- Shelf (COTS) (and potentially Government Off-The-Shelf (GOTS)) applications and their associated Application Programming Interfaces (APIs), and web applications. SDDB expects to implement and support various Open Source Software applications and additional platforms in the future. There is also the potential that a cloud computing environment could be introduced over the time frame of this contract. Along with the environment, these define the core skills required by the team on this contract; the following lists of skills demonstrate the breadth of the Team's knowledge requirements, but many additional skills may be needed as well for a maintenance developer to perform their day-to-day work. Potential future changes or additions to the environment are also noted.

Performance Objective 28: Software Support (Optional)

The contractor team shall support a software development procedure that follows EPA, OPP, and NIST policies.

Sub-Task A: Analysis, Design, & Development Services

The contractor team shall provide requirements analysis, design, and development services in support of software and system maintenance. The contractor team shall perform root-cause analysis on issues and record the root-cause from the analysis. The contractor team shall ensure source code is commented appropriately when significant code changes (changes to functionality or algorithms) are made. The contractor team shall ensure that bugs, data fixes, new (usually minor) features/enhancements, and tasks are performed in their appropriate priority order.

Sub-Task B: Commercial Off-The-Shelf/Open Source Software Product Implementation Services

The contractor team shall provide requirements analysis, design, and development services in support of software and system maintenance that includes Commercial Off-The-Shelf (COTS) and/or Open Source Software (OSS) products. The contractor team shall perform root-cause analysis on issues and record the root-cause from the analysis. The contractor team shall ensure source code or product configuration files are commented appropriately when significant code/configuration changes (changes to functionality or algorithms) are made. The contractor team shall ensure that bugs, data fixes, new (usually minor) features/enhancements, and tasks are performed in their appropriate priority order. Where code changes are actually within an OSS product, this code will be socialized and contributed back to the supporting OSS community.

Sub-Task C: Quality Assurance

These services shall increasingly involve Test Driven Development practices starting 3 months after award for languages, COTS/OSS products, and platforms that can support it; at that time, the contractor team shall provide reports of test coverage and metrics of pass/fail of unit tests. Within 6 months of contract award, the contractor shall provide automated functional tests that are suitable to replace manual user acceptance testing; these test results will be available for review. The contractor team will be expected to extend the tests to other forms of testing (e.g. performance, security) over the life of the contract. When selecting COTS or OSS products, the ability to perform TDD will be a consideration for selection.

Sub-Task D: Change/Configuration Management

The contractor team shall ensure all application source code, configuration files, and tests shall be checked into the source code repository daily. The contractor team shall properly update the statuses within the issue tracking). The contractor team shall tag and manage releases including appropriate branching and merging back to the trunk of the application source code.

Sub-Task E: System Development Life-Cycle Documentation

The contractor team shall update appropriate system life-cycle documentation and ensure it is completed within 5 days of a production release.

Quality Assurance Surveillance Plan for Performance Objective 28

Performance Objectives	Performance Measures	Performance Standards Target	Surveillance Plan	Contractor Incentive
Performance Object 28 Software Maintenance Support				
1) Analysis, Design, & Development/	Maintenance Tickets/Issues	For Maintenance Tickets/Issues, root- cause analysis is performed and documented in the issue tracking system 95% of the time.	Random sampling of the issue tracking system. Notification in writing of non-compliance upon discovery.	1) Please see page 7.

Performance Objectives	Performance Measures	Performance Standards Target	Surveillance Plan	Contractor Incentive
Performance Object 28 Software Maintenance Support				
2) Quality Assurance	Provide unit tests	For enhancements and maintenance development projects, 99% of all Critical or Major Severity issues are documented and caught before being released to functional user acceptance testing.	Random samples of unit test coverage report compared to issue tracking system. Notification in writing of non-compliance upon discovery.	2) Please see page 7.
3) Change/Configuration Management	Provide user acceptance tests Code checked-in	For enhancements and maintenance development projects, 90% of all other Severity/Priority issues are	Random samples of unit test coverage report compared to issue	3) Please see page 7.

		documented and caught before being released to functional user acceptance testing.	tracking system. Notification in writing of non-compliance upon discovery.	
		Provide functional user acceptance testing on must-have features with test coverage of at least 60%; this coverage should improve over the contract.	User acceptance test coverage report compared to requirements life-cycle documentation. Notification in writing of non-compliance upon discovery.	
		All source code changes checked in at least daily.	Direct observation and random sampling of source code repository. Notification in writing of non-compliance upon discovery.	
	Tests checked-in	All unit tests are a part of the source code and checked in at least daily 95% of the time.	Direct observation and random sampling of source code repository.	

Performance Objectives	Performance Measures	Performance Standards Target	Surveillance Plan	Contractor Incentive
Performance Object 28 Software Maintenance Support				
			Notification in writing of non-compliance upon discovery.	
		All functional user acceptance tests checked in at least daily 95% of the time.	Direct observation and random sampling of source code repository. Notification in writing of non-compliance upon discovery.	Please see page 7.
4) SDLC Documentation	Issue tracking/ maintained Release baselines managed	Issues and their associated categories and statuses are maintained with 95% accuracy.	Direct observation and random sampling of issue tracking system. Notification in writing of non-compliance upon discovery.	4) Please see page 7.
		All source code (including configuration for data files), life-cycle documentation (if updated), unit tests, and functional user acceptance tests are tagged with their release and	Random sampling of life- cycle documentation and source code repository. Notification in writing of non-compliance upon discovery.	

		promoted 95% of the time.		
	SDLC documentation maintained	Life-cycle documentation and/or documentation updates completed within 5 days of production release date.	Random sampling of life- cycle documentation. Notification in writing of non-compliance upon discovery.	

NOTE: Notification in writing could be in the form of email. Additionally, all financial penalties or awards above could also have negative or positive comments made into CPARS.

Performance Objective 29: New System Development (Optional)

Under this objective the contractor shall be required to perform any or all of the tasks associated with the development of new information systems to include workgroup support; requirements analysis; design; prototyping; development; testing; implementation, transition, and warranty support; and training. All work shall follow EPA, OPP, and other Federal policies and procedures as instructed by the TOCOR/ATOCORs. The contractor will manage the new development projects using an Agile Development methodology; vendors are encouraged to use CMMI Level III best practices, but this is not required. Even though the particulars of each order will vary, basic functions are expected to be included in each.

Sub-Task A: Analysis, Design, & Development Services

The contractor shall provide workgroup support, requirements analysis, design, and development services in support of software and system development. Workgroup support may include creating agendas, taking meeting minutes/notes, or facilitation as required in the specific task order objectives.

Sub-Task B: Quality Assurance

The contractor shall provide, as appropriate for each task order, proper quality assurance processes and controls. All source code shall be adequately tested and be bug-free upon final delivery to the EPA. The contractor shall ensure source code is commented appropriately and that all required documentation is delivered on-time and within acceptable quality standards.

Sub-Task C: Change/Configuration Management

The contractor will ensure all application source code, configuration files, and tests shall be checked into the source code repository upon delivery to the TOCOR/ATOCOR. The contractor shall tag and manage releases including appropriate branching and merging back to the trunk of the application source code.

Sub-Task D: System Development Life-Cycle, Training, and other Required Documentation

The contractor shall update appropriate system life-cycle documentation and ensure it is completed within the timeframe specified in the task order and agreed to by the TOCOR/ATOCOR. All other documentation, training materials, and/or presentations shall be delivered in accordance with the task order objectives and requirements.

Sub-Task E: Provide transition support to the Maintenance Team

The contractor, when appropriate, will interact with and provide transition support to the SDDB maintenance team or other staff as directed by the TOCOR/ATOCOR. Interactions will include but not be limited to consultations, planning meetings, and new development hand-off support. The contractor shall provide a warranty period as specified in the particular task order.

Quality Assurance Surveillance Plan for Performance Objective 29

Performance Objectives	Performance Measures	Performance Standards Target	Surveillance Plan	Contractor Incentive
Performance Object 29: New System Development				
1) Analysis, design, & development Services	All deliverables and documents relevant to each task of this Objective (including notes, agendas, etc.) are stored in the CM tool.	100% (one hundred percent) of deliverables and SDLC documents are stored in CM tool	1) Direct observation and random sampling. The Contractor shall be alerted, in writing, whenever performance objectives are not achieved. 2) Daily stand-up & random sampling of the issue tracking system. Notification in writing of non-compliance upon discovery.	1) Please see page 7.

2) Quality Assurance	Provide unit tests	1) For frameworks/environments where supported, test coverage should be a minimum of 30% and continually improve over the contract. 2) For enhancements and maintenance development projects, 99% of all Critical or Major Severity issues are documented and caught before being released to functional user acceptance testing. 3) For enhancements and maintenance development projects, 90% of all other Severity/Priority issues are documented and caught before being released to functional user acceptance testing. 4) Test coverage reported with 99% accuracy.	Unit test coverage report. Notification in writing of non-compliance upon discovery. 2) Random samples of unit test coverage report compared to issue tracking system. Notification in writing of non-compliance upon discovery. 3) Random samples of unit test coverage report compared to issue tracking system. Notification in writing of non-compliance upon discovery. 4) Random sampling of source code repository compared to coverage reports. Notification in writing of non-compliance upon discovery.	2) Please see page 7.

	Provide user acceptance tests	1) Provide functional user acceptance testing on must-have features with test coverage of at least 60%; this coverage should improve over the contract.	1) User acceptance test coverage report compared to requirements life-cycle documentation. Notification in writing of non-compliance upon discovery.	1) The Contractor will be penalized 10% (ten percent) of the invoiced amount for the current billing cycle of that performance objective for three (3) or more written warnings of inadequate deliverable quality throughout the performance period. 1) The Contractor will be penalized 1% (one percent) of the invoiced amount for the current billing cycle for each instance of untimely delivery.

3) ange/Configuration Management	1) All deliverables and documents relevant to each Task Objective (including notes, agendas, test scripts, code, etc.) are stored in the CM tool.	1) 100% (one hundred percent) of deliverables and documents are stored in CM tool. All unit tests are a part of the source code and checked in at least daily 95% of the time. All source code checked in at least daily.	1) Direct observation and random sampling. The Contractor shall be alerted, in writing, whenever performance objectives are not achieved.	3) Please see page 7.

	2) Issue tracking maintained	2) Issues and their associated categories and statuses are maintained with 95% accuracy.	2) Direct observation and random sampling. The Contractor shall be alerted, in writing, whenever performance objectives are not achieved.	
4) SDLC Documentation	1) SDLC documentation maintained	1) Life-cycle documentation and/or documentation updates completed within 5 days of production release date.	1) Random sampling of life-cycle documentation. Notification in writing of non-compliance.	Please see page 7.

NOTE: Notification in writing could be in the form of email. Additionally, all financial incentives and disincentives awarded throughout the life of the task order could be documented in the annual evaluation of contractor performance that is entered into CPARS.

Performance Objective 30: Web Site Support/Application Development (Optional)

To effectively perform the work outlined in this contract, the Contractor will be required to provide a wide range of internet and intranet web site support, to include analysis, development, and enhancement to web applications (i.e. ColdFusion, Oracle, PHP, MySQL, APEX etc.) using Agency supported and approved software. In addition, the Contractor will be required to develop tools and electronic applications to manage the large volume of data and information that will be generated. This section of the contract addresses tasks that are specific to the Office of Pesticide Programs (OPP) under this contract. The following tasks are required:

Sub-Task A: OPP Internet/Intranet Web Site Maintenance and Support

Maintenance

The contractor shall provide reports to identify potential web site problem areas. Agency reports shall be used to assist with the correction of any identified dependencies and supplement contractor generated reports. Redundant, outdated, and trivial (ROT) web content identified in Agency or contractor generated reports shall be archived and removed as directed by OPP.

The contractor shall conduct and review quality assurance and control measures to ensure data and information are accurate and up to date. Proper quality assurance and quality control documentation shall be prepared and maintained by the contractor.

Support

The contractor shall review and assess evolving Agency web requirements and recommendations and propose an implementation plan/strategy for retrofitting the current OPP web structure to meet new Agency requirements.

The contractor shall propose recommendations for the development, improvement, enhancement, and user testing of the Pesticides web site to include design/redesign (i.e. navigation, content consolidation), organization (i.e. Information Architecture, taxonomy, and metadata), aesthetics, and appropriateness to targeted audience. The contractor shall assist with implementing the proposed recommendations as directed by OPP.

Web pages shall be produced and implement for new and existing web content as directed by OPP.

Deliverables for Sub-Task A: OPP Internet/Intranet Web Site Support and Maintenance

Provide Monthly Reports to address the following:

Service Reports

- Confirm site connectivity via the Internet once per business day.
- Check all active links and form pages on the site to ensure they are functioning properly once per month, and not later than the 4th Friday in the business month.

- **Metadata Reports**
  Identify PDF and HTML files that are missing metadata.

- Review Pesticides web site content inventory, Maxamine and Rotweiller Reports.

- Remove duplicate files identified in the web content inventory reports.

- Identify and delete outdated image files.

- Check and repair broken links identified in the Maxamine reports.

- Leverage tools such as PreTidy to clean errors in HTML code.

- Check alternate language pages (e.g., Spanish) for improper HTML entities.

- Keep the Pesticides web site in compliance with the EPA Procedures, Standards and Guidance (http://yosemite.epa.gov/oei/webguide.nsf/standards-guidance)/CIO ADA 508 standards.

- Keep site refreshed with information provided by OPP ITB.

- Respond to all work requests for web site maintenance actions with an email within 3 hours of the request confirming your understanding or request for clarification prior to beginning work on the request.

Sub-Task B: Web Site Management Improvements

The contractor shall participate in the design and development of web content management capabilities using web content management system (WCMS) software including but not limited to Drupal and Documentum CMS. Prior to WCMS selection, the contractor shall work with OPP to develop technical requirements for the development of a WCMS environment. In order to customize the WCMS system, the contractor shall architect WCMS solutions by researching, evaluating, and recommending modules; guiding staff in defining taxonomies, content types, permissions and groups. The contractor will assist in designing, building, and developing web sites for internal stakeholders in the WCMS environment, including adding contributed modules and customizing themes.

The contractor shall transfer existing internet and intranet web content into a WCMS. The contractor shall oversee and perform upgrades to the WCMS infrastructure.

Deliverables for Sub-Task B: Web Site Management Improvements

- Design, develop and implement a WCMS that meets the technical requirements set forth by the TOCOR.
- Customize WCMS (including but not limited to Drupal, Documentum) to meet the needs of OPP.
- Develop web content migration strategy and approach, define scope, schedule, resource plan, technical requirements and detailed execution plan.
- Develop migration routines and validate business equirements for historical data.
- Complete end-to-end migration in a sandbox environment.
- Execute full-scale migration into production environment.
- Present information and recommendation(s) on current patches/upgrades that should be applied to the WCMS infrastructure. Apply patches and ensure continued operation of the WCMS.
- Submit in writing to the CO and a copy to the TOCOR your request for contract modification for any development requests that would lead to a modification to existing contract terms.

Contractor shall not proceed to work on any modification that alters the terms of the contract or increases the scope of the contract without prior authorization of the Contracting Officer.

Sub-Task C: WCMS Training

The contractor shall provide on-the-job training and support to OPP staff involved with web content creation in the WCMS environment. The contractor shall be responsible for providing training materials to be utilized for future training provided by OPP.

Deliverables for C: WCMS Training

- Train the trainer sessions: The contractor shall provide at least two on-site 120-minute training sessions prior to web site content migration completion. These train the trainer sessions will include delivery of training curriculum plan and user documentation for use in subsequent end user training sessions.

Sub-Task D: OPPIN Integration and Web Application Development/Maintenance

Numerous web applications leverage chemical information originating from OPPIN. The contractor shall maintain and upgrade these existing web applications.

The contractor shall develop, design and build new web applications that will interface with OPPIN. The contractor shall develop processes to facilitate data transfer between new web applications and OPPIN. The contractor shall identify data quality issues by analyzing data residing in OPPIN or other OPP web applications. The contractor shall assist with developing strategies to integrate chemical information found throughout the current Pesticides web site and in various internal OPP applications into a web application.

Deliverables for D: OPPIN Integration and Web Application Development/Maintenance

- Contractor is to provide a minimum of (1) Software developer/architect as the principal developer and maintenance technician who possesses five or more years of extensive knowledge in the demonstrated development and deployment of APEX web applications. Additionally, a minimum of (1) Mid-level developer to support help-desk requests for assistance (for existing web applications) from users is also beneficial, but not required.

- For existing web applications, contractor will perform Tier 1 and Tier 2 maintenance functions (Tier 1 = basic admin to include password creations and resets, login access restore, base data manipulations, as directed, etc. Tier 2 = perform analysis of service failures and recommend solutions to fix, perform software updates, perform

directed upgrades to existing deployed software or transition to newer versions of software).

- Conduct contractor development briefings with OPP to detail approach to meeting the requirements of any requested new web application.

- Respond with the analysis to all requests for web application modification resulting from the issuance of an "OPP Work Request" in writing via email or faxed document.

- Respond to all work requests for maintenance via a web application update or change to existing function, feature or content w/ an email within 3 hours of the request confirming your understanding or request for clarification prior to beginning work on the request.

- Develop processes to enable sharing of OPPIN chemical information with OPP applications.

- Provide reports outlining data quality issues. These reports will allow OPP to easily identify data gaps and inaccurate information.

- Submit in writing to the CO and a copy to the TOCOR your request for contract modification for any development requests that would lead to a modification to existing contract terms.
- Contractor shall not proceed to work on any modification that alters the terms of the contract or increases the scope of the contract without prior authorization of the Contracting Officer.

Performance Objective 30: Program Management
Quality Assurance Surveillance Plan

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE (CI)
Performance Objective 30- Web Support/Application Development				
1) OPP Internet/Intranet Web Site Maintenance and Support	1) Review and develop monthly web reports. 2) Address Redundant, outdated, and trivial (ROT) web content. 3) Review and assess evolving Agency web requirements. 4) Propose Recommendations for the development, improvement and enhancement, and user testing of OPP web site. 5) Produce new web content. Update existing web content.	1) Documents are delivered on time; no more than five (5) typographical, spelling, and formatting errors identified in any draft or final document.	The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved. Adherence to the confirmation checks for all work requests for web site changes and/or updates. Successful execution/delivery of maintenance tasks.	1) Please see page 7.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE (CI)
Performance Objective 30- Web Support/Application Development				
2) Web Site Management Improvements	1) Design and develop web content management capabilities. 2) Develop technical requirements for the development of a WCMS environment. 3) Migrate existing internet and intranet web content into a WCMS. 4) Customize and upgrade WCMS environment.	1) Successful deployment of a WCMS. 2) Ensure no more than 10% rework of web content post web content migration into WCMS environment.	The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved. Adherence to the confirmation checks for all work requests for web site changes and/or updates. Successful execution/deliver y of maintenance tasks.	2) Please see page 7.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE (CI)
3)WCMS Training	1) Develop easy to read, reusable training materials. 2) Deliver two 120-minute training sessions prior to web content migration completion 3) Deliver up to two additional training sessions annually.	1) Deliver materials in a timely manner such that time is allowed for review and editing if needed. 2) Deliver training sessions before migration is completed. 3) Written deliverables must be in compliance with applicable standards, be clear, comprehensive, readable, and technically correct, show expertise, incorporate all features requested by TOCOR, and be appropriate for the targeted audience.	The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved. Adherence to the confirmation checks for all work requests for web site changes and/or updates. Successful execution/delivery of maintenance tasks.	3) Please see page 7.

PERFORMANCE OBJECTIVES	PERFORMANCE MEASURES (PM)	PERFORMANCE STANDARDS (PS) QA TARGET	SURVEILLANCE PLAN (SP)	CONTRACTOR INCENTIVE (CI)
4)PRISM Integration and Web Application Development/ Maintenance	1) Perform Tier 1 and Tier 2 maintenance on existing web applications. 2) Develop, design and build new web applications that interface with PRISM. 3) Develop processes to facilitate data transfer between new web applications and PRISM 4) Identify data quality issues in PRISM or other OPP web applications. 5) Develop strategies to integrate chemical information found throughout the current Pesticides web site and in various internal OPP applications into a web application.	1) Respond to all work requests for existing web application maintenance via a software update or change to existing function, feature or content w/ an email within 3 hours of the request confirming your understanding or request for clarification prior to beginning work on the request. 2) Successfully complete development and implementation of new web application that meet requirements set forth in the PWS or task document. 3) Provide task order or work request analysis per the guidance given in the task instructions.	The Contractor shall be alerted, in writing, whenever Performance Objectives are not achieved. Adherence to the confirmation checks for all work requests for web site changes and/or updates.	4) Please see page 7.

Acronyms

The table below contains a listing of acronyms used throughout this document.

Exhibit 1. ***Acronyms***

Acronym	Description
ACL	Access Control List
ATOCOR	Alternate Task Order Contract Officer Representative
AD	Active Directory
API	Application Programmable Interface
AS	Application Server
BOF	Business Object Framework
BPPD	Biopesticides and Pollution Prevention Division
TOCOR	Task Order Contract Officer Representative
CSIB	Customer Service & Infrastructure Branch
CSS	Cascading Style Sheet
DA	Documentum Administrator
DAO	Data Access Object
DCI	Data Call-In
DFC	Documentum Foundation Class
DOM	Document Object Model
DTO	Data Transfer Object
ECM	Enterprise Content Management
eCSF	Electronic Confidential Statement of Formula
eDPAF	Electronic Delivery Product Acceptance Form
EDSP	Endocrine Disruptor Screening Program
EFED	Environmental Fate and Effects Division
EPA	Environmental Protection Agency
ERD	Entity-Relationship Diagram
ESA	Endangered Species Act
EVM	Earned Value Management
FC	Fiber Channel
FIPS	Federal Information Processing Standards
FRD	Functional Requirements Document
FWS	U.S. Fish and Wildlife Service
GNIS	Geographic Names Information System
GUI	Graphical User Interface
HED	Health Effects Division
HQL	Hibernate SQL

HUC	Hydrologic Unit Code
IE	Internet Explorer
IoC	Inversion of Control
ITB	Internet & Training Branch
ITRMD	Information Technology and Resource Management Division
JDBC	Java Database Connectivity
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEI	Lotus Enterprise Integrator
LUIS	Label Use Information System
MD5	Message Digest Algorithm 5
MVC	Model – View – Controller
NGS	Nortel Government Solutions
NMFS	U.S. National Marine Fisheries Service
OGC	Office of General Counsel
OGNL	Object-Graph Navigation Layer
OO	Object-Oriented
OPP	Office of Pesticide Programs
OPPIN	Office of Pesticide Programs Information Network
OPPTS	Office of Pollution Prevention & Toxic Substances
PL/SQL	Programming Language/Structured Query Language
PPLS	Pesticide Product Label System
PRISM	Pesticide Registration Information SysteM
RDBMS	Relational Data Base Management System
RHEL	Red Hat Linux
SAN	Storage Area Network
SBO	Services Based Object
SDDB	Systems Design and Development Branch
SDK	Software Development Kit
SME	Subject Matter Expert
SOA	Service-Oriented Architecture
SQL	Standard Query Language
SSO	Single Sign-On
SSTS	Section Seven Tracking System
TESS	Threatened and Endangered Species System
UML	Unified Modeling Language
URI	Universal Resource Identifier
URL	Universal Resource Locator
USGS	United States Geological Survey

WDK	Web Development Kit
WSF	Web Services Framework
XML	eXtensible Markup Language

RESPONSIBILITIES OF THE CONTRACTOR

Work Plan and Deliverables

The Contractor shall produce work plans using Microsoft Project 2003 or higher. Documentation shall be prepared using Microsoft Word 2003 or higher and shall be delivered in hard copy on 8 /" X 11" paper and soft copy on CD. All System/application maintenance must be accompanied by an approved System Change Request (SCR). All Deliverables must be accompanied with a Deliverable Product Acceptance Form (DPAF) with the appropriate signatures. (see attached)

Standards for User Meeting and User Interviews

The Contractor shall provide meeting agendas at least two days prior to a scheduled meeting so that all Participants can prepare to contribute to the meeting process. The Contractor shall provide minutes of all user meetings and all user interviews within two days after the meeting.

Status Reporting

The Contractor shall apprise the Government TOCOR/ATOCOR of any problems throughout the contract life as they transpire. The contractor shall supply weekly status reports by the last day of each week identifying work accomplished during the period, work planned for the next period, and any problems resolved or unresolved.

Clearance Required: To perform the tasks necessary to fulfill the requirements of this contract, the contractor will require access to CBI data. A management control plan will be implemented to address the CBI, COI, and 508 Compliance issues in accordance with the following EPAAR clauses:

A) EPAAR 1552.235.73 (Access to FIFRA CBI)
B) EPAAR 1552.235.77 (Data Security – FIFRA CBI)
C) EPAAR 1552.209.71 (Organizational Conflict of Interest)
D) EPAAR 1552.209.73 (Notification of Conflicts of Interest Regarding Personnel)
E) EPAAR 1552.209.75 (Annual Certification)
F) EPAAR 1552.227.76 (Project Employee Confidentiality Agreement)
G) EPA 2100.1 and EPA 3110.21(a)(1) - 508 COMPLIANCE: All deliverables shall be in compliance with Section 508, Accessibility Standards of the Rehabilitation Act, of 1973 and Amendments of 1998. When preparing deliverables, the contractor shall refer to the most recent version of the 508 Standards at: http://www.access-board.gov/sec508/guide/.

Methodology for Work Tasks

All work performed by the contractor must adhere to the government policies guidance in the following manuals:

EPA EPAAR Manual -
http://oamintra.epa.gov/?q=node/5 EPA
Personal Computer Security Manual
OPP Quality Assurance Plan - Office of Pesticide Programs Quality Management Plan, Approved11/17/2006 OPP Risk Analysis – Risk Assessment for Office of Pesticide Programs Infrastructure Network (OPPIN Major Application, May 1, 2008
OPP Applications Security Plan – OPP Integrated PRISM Major Application System Security Plan, November 4, 2009
OPP LAN Security Plan
EPA Information Resources
Management Policies Manual EPA
Information Security Manual
EPA Operations and Maintenance Manual
EPA Systems Design &
Development Guidance
NDPD Operational
Policies Manual
OPP Standard Operating Procedures for the Development and Review of Publications: Printed, Web, and Other Media
EPA Web Guide
EPA Standard
Configuration Documents
(SCDs) EPA OEI
Guidance Documents
EPA Interim System
Lifecycle 7100.4
EPA FIFRA
Security Manual

Comply with EPA Policy for System Life Cycle Management (SLCM) Procedure; Classification No.: 2121-P-01.0 CIO Transmittal No.: 07-003, Approval Date 6-28-2007; Review Date: 06/2010

All the above manuals will be made available to the contractor through the EPA TOCOR/ATOCOR.

VI. INSPECTION AND ACCEPTANCE PROCEDURE/CRITERIA

Deliverables will be inspected/tested by EPA and will be accepted by the

TOCOR/ATOCOR when it is determined that software performs to specifications and is reliable or that other deliverables are complete and accurate and conform to OPP and EPA guidance.
Through an iterative process, the EPA TOCOR/ATOCOR develops detailed system requirements and specifications documents and works with the Contractor Project Manager to develop a project schedule. The detailed specifications document will describe screens, navigation and interface among screens, data validation rules, and detailed storage and processing requirements.

Software acceptance is based on error free testing in the "beta test" with the software meeting all of the criteria in the design specifications and sign off acceptance by the TOCOR/ATOCOR. A review with the TOCOR/ATOCOR and other EPA personnel as necessary with signatures on a DPAF will lead to final acceptance.

Non-software deliverables will be accepted in writing by the TOCOR/ATOCOR. The non-software deliverables will be judged complete if they are correct, error free, and fully meet the design specifications as presented inwriting to the contractor.

VII. REPORTING REQUIREMENTS

The contractor shall produce standard delivery order reports, plus a monthly report, to be submitted within five (5) working days after the close of the contractor invoice cycle, to consist of the hours worked, and a summary of the progress toward the completion of all requirements of the contract. This shall include current month data, as well as year-to-date data in both hours/dollars.

VIII. Labor Mix

The technical skills and educational requirements identified in this PWS are strongly recommended and/ preferred.

IX. SECURITY, CONFIDENTIAL BUISINESS INFORMATION, PRIVACY ACT AND TRAINING

All contract employees must meet the personnel security requirements to receive an EPA Personnel Access and Security System (EPASS) badge. Requirements are further defined in the clauses of this contract.

Contractors shall complete mandatory role-based IT Security and Privacy Awareness Training upon employment. These trainings cover Environmental Protection Agency (EPA) policy on how to identify, report, handle and protect Confidential Business Information (CBI) and Personal Identifiable Information (PII) properly. All federal employees and contractors are required to complete their privacy and security awareness training each year. These courses are intended to enforce the importance and apply policies on protecting PII and CBI for users with significant information privacy responsibilities such as, privileged account holders or those with access to sensitive PII and CBI.

Completion of the course is tracked. To be considered as completed, each user must

correctly answer all knowledge-based questions. The Contractor shall print the certificate of completion and shall submit it to their Project Manager and Task Order Contracting Officer Representative (TOCOR) for recordkeeping purposes.

Contract employees must complete Confidential Business Information (CBI) training prior to receiving access to OPP's physical and logical spaces, as well as, limited required annual training such as computer security training. All contractors and subcontractors shall be subject to clearance for the handling of CBI per the *FIFRA Information Security Manua*l and Toxic Substances Control Act (TSCA) CBI 14(d) of TSCA (15 USC 2513(d)).

The Contractor shall implement a management control plan that will address the CBI, COI, and 508 Compliance issues in accordance with the following EPAAR clauses:

1) EPAAR 1552.235.73 (Access to FIFRA CBI)
2) EPAAR 1552.235.77 (Data Security – FIFRA CBI)
3) EPAAR 1552.209.71 (Organizational Conflict of Interest)
4) EPAAR 1552.209.73 (Notification of Conflicts of Interest Regarding Personnel)
5) EPAAR 1552.209.75 (Annual Certification)
6) EPAAR 1552.227.76 (Project Employee Confidentiality Agreement)

All contractors and subcontractors shall adhere to FAR 52.224-1 Privacy Act Notification, EPAAR 48 CFR Subpart 24.104. The Contractor agrees to comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the Task specifically identifies systems of records; and design, development, or operation work that the Contractor is to perform.

Privacy Act Notification (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

Information Security Requirements:

All work that is associated with government information, systems, and information security must be in compliance with the Federal Information Security Modernization Act of 2014 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "Minimum Security Requirements for Federal Information and Information Systems." This standard specifies minimum-security requirements Federal agencies must meet. The appropriate security controls and assurance requirements to be selected are described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" and associated documents. Specific impact levels required (per FIPS 200) for government information and information systems may vary and will be specified as requirements are identified.

The following Notice, interim policy notice (IPN #17-01), provides guidance on using the attached limited-use cybersecurity tasks (22) that need to be adhered too as part of this performance work statements (PWS) should they apply.

Cybersecurity and Protecting Sensitive Information

The tasks which are applicable to this requirement are indicated below:

Task	Title	Applicable
A	Personally, Identifiable Information Contract Closeout	☒
B	Contractor Return of all EPA-Provided and EPA-Activity-Related Information	☒
C	Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information	☒
D	Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment	☒
E	Authority to Operate (ATO) Suspension or Revocation	☒
F	Security Monitoring and Alerting Requirements	☒
G	IT Security and Privacy Awareness Training	☒
H	Specialized Information Security Training for Staff with Significant Security Responsibilities	☒
I	Federal Reporting Requirements	☒
J	Protecting Sensitive Information	☒
K	Security Assessment and Authorization (SA&A)	☒
L	Contractor System Oversight/Compliance	☒
M	Contractor Access to EPA IT Systems	☒
N	Individual Notification for Personally Identifiable Information	☒
O	Credit Monitoring and Identity Protection	☒
P	Compliance with IT Security Policies	☒
Q	Secure Technical Implementation	☒
R	Internet Protocol Version 6 (IPv6)	☒
S	Cloud Service Computing	☒
T	Contract Performance Information and Testimony	☒
U	Rehabilitation Act Section 508 Standards	☒
V	Termination for Default - Failure to Report Information Security Incident	☒

Task Key:

Requirement Type	Required Tasks
IT Hardware	A,B,C,F,G,H,I,J,K,M,P,Q,R,T,U,V
IT Software	A,F,H,I,J,K,L,M,P,Q,R,T,U,V
Green IT	A,B,C,E,F,H,I,J,K,M,P,Q,R,U,V
IT Services	A,B,C,D,E,G,H,I,J,L,M,O,P,Q,T,U,V
Data Center Services	A,B,C,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,T,U,V

Cloud Computing	A,B,C,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V
Cyber Security Product and Services	A,B,E,F,G,H,I,J,K,L,M,O,P,Q,R,T,V

The full text of the tasks are described, as follows:

Task A - Personally Identifiable Information Contract Closeout

(a) *Definition.* Personally Identifiable Information (PII) - as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, PII refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

(b) *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information (including but not limited to all records, files, and metadata in electronic or hardcopy format).* As part of contract closeout, the Contractor shall submit a *Certification of Sanitization of EPA-provided and EPA-Activity-Related Files and Information* to the Contracting Officer and the Task Order Contracting Officer's Representative (TOCOR) following the template provided in Appendix G of National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization Revision 1*, which assesses risk associated with Personally Identifiable Information (PII) that was generated, maintained, transmitted, stored or processed by the Contractor. The Senior Agency Official for Privacy (SAOP) shall review the Certification and coordinate with the Contracting Officer and the TOCOR.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task B - Contractor Return of all EPA-Provided and EPA-Activity-Related Information

(a) Within thirty (30) days (or a different time period approved by EPA) of an EPA request, or after the end of the contract performance period, the Contractor must return all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must return originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Contractors must return all originals so that they cannot be used for further business by Contractor.

(b) Concurrent with the return of all originals as set forth in paragraph (a), the Contractor must document to the EPA the return of all originals of all EPA-provided and EPA-Activity-Related Information (including but not limited to all records, files, and metadata in electronic or hardcopy format). The Contractor must document originals obtained while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or

received from the Contractor by any other related organization and/or any other component or separate business entity.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task C - Verified Secure Destruction of All EPA-Provided and EPA-Activity-Related Information

(a) Within 60 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must execute secure destruction (either by the Contractor or third-party firm approved in advance by EPA) of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related files and information (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

(b) Within 75 days after the end of the contract performance period or a time period approved by EPA, or after the contract is suspended or terminated by EPA for any reason, and after EPA has accepted and approved the Contractor's return of information, the Contractor must document to the EPA the secure destruction of all existing active and archived originals and/or copies of all EPA-provided and EPA-activity-related files and information, (including but not limited to all records, files, and metadata in electronic or hardcopy format). This information includes but is not limited to information obtained by the Contractor while conducting activities in accordance with the contract with EPA; or distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or received from the Contractor by any other related organization and/or any other component or separate business entity. Destruction Methods shall be by procedures approved by EPA in advance in writing.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task D - Contractor Return of all EPA-Owned and Leased Computing and Information Storage Equipment

(a) Within 60 days (or a different time period approved by EPA) after the end of the contract performance period, the Contractor must return all EPA-owned and leased computing and information storage equipment to EPA.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task E - Authority to Operate (ATO) Suspension or Revocation

(a) *Definitions*.

(i) Authority to Operate (ATO) - Signed by the Agency chief information officer (CIO) or deputy CIO, ATOs are issued for all information systems that input, store, process, and/or output Government information. In order to be granted an ATO, all federal information systems must be compliant with National Institute of Standard and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, instead of NIST SP 800-53.

(ii) Information Security Incident - an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(iii) Sensitive Information - As defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

(b) In the event of an Information Security Incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this requirement, the Contracting Officer may direct the Contractor to take additional security measures to secure Sensitive Information. These measures may include restricting access to Sensitive Information on the Contractor information technology (IT) system under this contract. Restricting access may include disconnecting the system processing, storing, or

transmitting the Sensitive Information from the Internet or other networks or applying additional security controls.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task F - Security Monitoring and Alerting Requirements

(a) All Contractor-operated systems that use or store EPA information must meet or exceed EPA policy requirements pertaining to security monitoring and alerting. All systems are subject to the requirements of existing federal law, policy, regulation and guidance (e.g., Federal Information Security Management Act of 2002). The Contractor must comply with the EPA-used Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) policy for security monitoring and alerting, which includes requirements not limited to:

(1) System and Network Visibility and Policy Enforcement at the following levels:

(i) Edge
(ii) Server / Host
(iii) Workstation / Laptop / Client
(iv) Network
(v) Application
(vi) Database
(vii) Storage
(viii) User

(2) Alerting and Monitoring

(3) System, User, and Data Segmentation

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task G - IT Security and Privacy Awareness Training

(a) The Contractor must ensure that all Contractor personnel complete EPA-provided mandatory security and privacy training prior to gaining access to EPA information systems. Non-compliance may result in denial of system access.

(b) The Contractor must ensure that all Contractor personnel complete security and privacy refresher training on an annual basis. EPA will provide notification and instructions to the Contractor on completing this training.

(c) The Contractor must ensure that each Contractor employee review and sign the *EPA Rules of*

Behavior pertaining to appropriate use of EPA information systems prior to gaining access to EPA information systems. The Contractor must also ensure that each Contractor employee reviews these *EPA Rules of Behavior* at least annually. EPA will provide notification to the Contractor when these reviews are required.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task H - Specialized Information Security Training for Staff with Significant Security Responsibilities

(a) The Contractor must ensure that Contractor personnel with significant information security responsibilities complete specialized information security training based on the requirements defined in the EPA role-based training program *(program provided after Contract award)*. The objective of the information security role-based training is to develop an EPA information security workforce with a common understanding of the concepts, principles, and applications of information security to ensure the confidentiality, integrity and availability of EPA's information and information systems. The Contractor is required to report training completed to ensure competencies are addressed. The Contractor must ensure employee training hours are satisfied in accordance with EPA Security and Privacy Training Standards *(provided after Contract award)*. The Task Order Contracting Officer's Representative (TOCOR) will provide additional information for specialized information security training based on the requirements in paragraph (b).

(b) The following role-based requirements are provided:

[Program office adds role-based requirements; otherwise write "none" or "not applicable"]

(c) The Contractor must ensure that all IT and Information Security personnel receive the necessary technical (for example, operating system, network, security management, and system administration) and security training to carry out their duties and maintain certifications.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task I - Federal Reporting Requirements

(a) Contractors operating information systems on behalf of EPA must comply with Federal Information Security Modernization Act (FISMA) 44 USC Section 3541 reporting requirements. Annual and quarterly data collection will be coordinated by EPA. Contractors must provide EPA with the requested information based on the timeframes provided with each request. Contractor systems must comply with monthly data feed requirements as coordinated by EPA. Reporting requirements are determined by the Office of Management and Budget (OMB), and may change for each reporting period. The Contractor will provide the EPA Task

Order Contracting Officer's Representative (TOCOR) with all information to fully satisfy FISMA reporting requirements for Contractor systems.

(b) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task J - Protecting Sensitive Information

(a) Definitions.

(1) Sensitive Information.

As defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sensitive Information is any information where the loss, misuse or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Sensitive Information is subject to stricter handling requirements than non-sensitive information because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

(2) Personally Identifiable Information (PII).

PII, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) Sensitive PII.

Sensitive PII refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than

PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) Authorization to Use, Store, or Share Sensitive Information.

(1) Through the Contracting Officer, the Contractor must obtain written approval by the Chief Information Officer (CIO) or designee prior to the use or storage of EPA Sensitive Information, or sharing of EPA Sensitive Information by the Contractor with any subcontractor, person, or entity other than the EPA.

(2) The Contractor shall not remove Sensitive Information from approved location(s), electronic device(s), or other storage systems, without prior approval of the CIO or designee obtained through the Contracting Officer.

(c) Information Types. Sensitive Information includes PII, which in turn includes Sensitive PII. Therefore all requirements for Sensitive Information apply to PII and Sensitive PII, and all requirements for PII apply to Sensitive PII.

(d) Information Security Incidents. An *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The Contractor must report all known Information Security Incidents if they involve Sensitive Information.

(1) Information Security Reporting Requirements.

(i) The Contractor must report all Information Security Incidents and Privacy Breaches in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. An information security report shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for Sensitive Information or has otherwise failed to meet contract requirements.

(ii) The Contractor must report via email all Information Security Incidents and Privacy Breaches to the EPA Service Helpdesk immediately, but not later than 30 minutes, after becoming aware of the Incident. The Contractor shall email the EPA Service Helpdesk at CSIRC@epa.gov, and shall also email the Contracting Officer and Task Order Contracting Officer Representative (TOCOR). If the Contractor fails to report in 30 minutes, specific Government remedies may include termination in accordance with EPA

Requirement *Termination for Default – Failure to Report Information Security Incident*.

(iii) The types of information required in an Information Security Incident and Privacy Breach reports include: Contractor name and point-of-contact (POC) information, Contract number; the type, amount and description of information compromised; and incident details such as location, date, method of compromise, and impact, if known.

(iv) The Contractor shall not include any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, the Contractor shall use Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information in attachments to email.

(v) If applicable, the Contractor must also provide supplemental information or reports related to a previously reported incident directly to the Contracting Officer, TOCOR and EPA Service Helpdesk at CSIRC@epa.gov. The Contractor shall include any related ticket numbers in the subject line of the email.

(2) Information Security Incident Response Requirements.

(i) All determinations related to Information Security Incidents and Privacy Breaches, including response activities, notifications to affected individuals and related services (e.g., credit monitoring and identity protection) will be made in writing by authorized EPA officials at EPA's discretion and communicated by the Contracting Officer.

(ii) The Contractor must provide full access and cooperation for all activities determined by EPA to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents. The Contractor shall maintain the capabilities to: determine what sensitive information was or could have been accessed and by whom, construct a timeline of user activity, determine methods or techniques used to access the information, identify the initial attack vector, and remediate and restore the protection of information. The Contractor is required to preserve all data, records, logs and other evidence that are reasonably necessary to conduct a thorough investigation of the Information Security Incident.

(iii) The Contractor is responsible for performing Incident and Privacy Breach Response activities required by EPA, including but not limited to inspections, investigations, forensic reviews, data analyses and processing by EPA and EPA OIG personnel and others on behalf of EPA. As requested by the Contracting Officer, the Contractor may provide technical support for the Government's final determinations of responsibility activities for the Incident and/or liability activities for any additional Incident Response activities (e.g., possible restitution calculation to affected individuals).

(iv) EPA, at its sole discretion, may obtain the assistance of Federal agencies and/or third-party firms to aid in Incident Response activities.

(v) The Contractor is responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by EPA.

(e) Contractor Plan for Protection of Sensitive Information. The Contractor is responsible for

the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Upon contract award, the Contractor shall develop and maintain a documentation plan addressing the following minimum requirements regarding the protection and handling of Sensitive Information:

(1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.

(2) Proper control and storage of mobile technology, portable data storage devices, and communication devices.

(3) Proper use of Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules to protect Sensitive Information while at rest and in transit throughout EPA, Contractor, and/or subcontractor networks, and on host and client platforms.

(4) Proper use of FIPS 140-2 compliant encryption modules to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

(5) Information Security Incidents. The Contractor shall report to the Government any security incident involving Personally Identifiable Information (PII) of which it becomes aware.

(6) Contractor Access to EPA IT Systems. The Contractor shall configure their network to support access to government systems (e.g., configure ports and protocols for access).

(a) Requirement for Business to Government (B2G) network connectivity. The Contractor will connect to the B2G gateway via a Contractor-procured Internet Service Provider (ISP) connection and assume all responsibilities for establishing and maintaining their connectivity to the B2G gateway. This will include acquiring and maintaining the circuit to the B2G gateway and acquiring a FIPS-140-2 Virtual Private Network (VPN)/Firewall device compatible with the Agency's VPN device. Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the Contractor.

(b) Dial-Up ISP Connections are not acceptable.

(c) The Contractor must comply with the Agency's Guidance regarding allowable ports, protocols and risk mitigation strategies (e.g. File Transfer Protocol or Telnet).

(7) IT Security and Privacy Awareness Training. The Contractor must ensure annual security education, training, and awareness programs are conducted for their employees performing under the subject contract that addresses, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering for their employees. The Contractor must also ensure employees performing under the subject contract receive the Agency's initial and annual information security awareness training.

(8) The Contractor must not conduct default installations of "out of the box" configurations of Commercially Off the Shelf (COTS) purchased products. The contractor shall configure COTS products in accordance with EPA, NIST, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) or Center for Internet Security (CIS) standards. Standards are listed in order of precedence for use. If standards do not exist from one of these sources, the contractor shall coordinate with EPA to develop a configuration.

(f) *Subcontract flowdown*. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task K - Security Assessment and Authorization (SA&A)

(a) The Contractor is required to undergo Security Assessment and Authorization (SA&A); i.e., the process by which a federal agency examines its information technology infrastructure and develops supporting evidence necessary for security assurance accreditation, prior to using information systems to access and/or store Government information, potentially including Sensitive Information. The Contractor's facilities must also meet the security requirements for "moderate confidentiality impact" as defined by the Federal Information Processing Standards (FIPS) 199 publication *Standards for Security Categorization of Federal Information and Information Systems*.

(b) For all information systems that will input, store, process, and/or output Government information, the contractor shall obtain an Authorization to Operate (ATO) signed by the Chief Information Officer (CIO) from the Contracting Officer (working with the Task Order Contracting Officer's Representative (TOCOR)) before using EPA information in the system. The contractor may be able to obtain an Authorization to Test from the SIO for the office obtaining services that will allow use of EPA information in certain circumstances to facilitate system development or implementation. Before a federal information system can be granted an ATO, it must be compliant with National Institute of Standard and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. Contractors whose internal information systems will process Sensitive Information incidental to Agency product or service development must meet requirements for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (instead of NIST SP 800-53) in order to be granted an ATO.

(c) FIPS 199 moderate confidentiality impact must be utilized for Contractor information technology (IT) systems and security control baseline requirements.

(d) Prior to Agency SA&A activities, the TOCOR must complete a Privacy Threshold Analysis (PTA) for all IT systems. Then the TOCOR must provide the completed PTA to the EPA Privacy Officer for a determination of whether a Privacy Impact Assessment (PIA) is required. If a determination is made that a PIA is required, it will be completed by EPA in accordance with EPA PIA Template instructions.

(e) The Contractor is responsible for preparing SA&A documentation with the use of EPA tools and security documentation templates including System Security Plan, Security Assessment Report, Contingency Plan, and Incident Response Plan. The Contractor must follow federally mandated SA&A and Risk Management Framework (RMF) processes throughout the IT system lifecycle process to ensure proper oversight by EPA. RMF modifies the traditional Certification and Accreditation process and integrates information security and risk management activities into the system development life cycle.

(f) The Contractor must submit SA&A documentation as defined in paragraph (e) to the TOCOR at least 60 days before the ATO expiration date.

(g) The Contractor shall fix or mitigate system or security vulnerabilities within a time frame commensurate with the level of risk (as identified by the EPA and Contractor) they present:

- High Risk = 2 business days from vulnerability notification from contractor
- Moderate Risk = 7 business days from vulnerability notification from contractor
- Low Risk = 30 business days from vulnerability notification from contractor

(h) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task L - Contractor System Oversight/Compliance

(a) Pursuant to National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev 4, the EPA and GAO have the authority to conduct site reviews for compliance validation and will conduct security reviews on a periodic and event-driven basis for the life of the contract. Full cooperation by the Contractor is required for audits and forensics.

(b) The Contractor shall provide EPA access to the Contractor's facilities, installations, operations, documentation, databases, information technology (IT) systems and devices, and personnel used in performance of the contract, regardless of the location. The Contractor shall provide access to the extent required, in EPA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of agency data or to the function of information technology systems operated on behalf of agency, and to preserve evidence of information security incidents. This information shall be available to the EPA upon request.

(c) All Contractor systems used in the performance of the contract must comply with Information Security Continuous Monitoring (ISCM) and Reporting as identified in OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*. In addition, EPA reserves the right to perform ISCM and IT security scanning of Contractor systems with tools and infrastructure of EPA's choosing.

(d) All Contractor systems used in the performance of the contract must perform monthly

vulnerability scanning as defined by EPA IT and Security Policy, and the Contractor must provide scanning reports to the Contracting Officer, who will forward them to the EPA CIO or designee on a monthly basis.

(e) All Contractor systems used in the performance of the contract must participate in the implementation of automated security controls testing mechanisms and provide automated test results in Security Compliant Automation Protocol (SCAP) compliant data to the Contracting Officer, who will forward to the EPA CIO or designee on a monthly basis.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task M - Contractor Access to EPA IT Systems

(a) Immediately following contract award, the Contractor shall provide to the Task Order Contracting Officer's Representative (TOCOR) a complete list of Contractor employee names that require access to EPA information systems.

(b) The Contractor shall provide a Contractor employee change report by the fifth day of each month after contract award to the TOCOR. The report shall contain the listing of all Contractor employees who separated or were hired under the contract in the past 60 days. This report shall be submitted even if no separations or hires have occurred during this period. Failure to submit a Contractor employee change report may, at the Government's discretion, result in the suspension of all network accounts associated with this contract. The format for this report will be provided by the TOCOR.

(c) (1) The Contractor shall require each of its employees who will need system access for six months or less to utilize a Personal Identity Verification-Interoperable (PIV-I) card or equivalent, as determined by EPA, in order to access EPA information technology (IT) systems and Sensitive Information. The Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

(2) The Contractor shall require each of its employees who will need system access for more than six months to utilize an HSPD-12 compliant Personal Identity Verification (PIV) card, such as the EPA EPASS card, in order to access EPA IT systems and Sensitive Information. The Contractor shall ensure that its employees complete a federal government-initiated background investigation as part of the PIV issuance process. The Contractor shall ensure that its employees will not share accounts to access EPA IT systems and Sensitive Information.

(d) EPA, at its discretion, may suspend or terminate Contractor access to any systems, information/data, and/or facilities when an Information Security Incident or other electronic access violation, use or misuse issue warrants such action. The suspension or termination shall last until EPA determines that the situation has been corrected or no longer exists. Upon request by EPA, the Contractor shall immediately return all EPA information/data, as well as any media

type that houses or stores Government information.

(e) The Contractor shall notify the TOCOR at least five days prior to a Contractor employee being removed from a contract (notification shall be at least 15 days for key personnel in accordance with requirement 1552.237-72, *Key Personnel*). For unplanned terminations or removals of Contractor employees from the Contractor organization that occur with less than five days notice, the Contractor shall notify the TOCOR immediately. The Contractor shall ensure that HSPD-12/PIV cards issued to a Contractor's employee shall be returned to the TOCOR prior to the employee's departure.

(f) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task N - Individual Notification for Personally Identifiable Information

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) The Contractor shall have in place procedures and the capability to notify any individual whose Personally Identifiable Information (PII) resided in the Contractor information technology (IT) system at the time of an Information Security Incident not later than five business days after being directed by the Contracting Officer to notify individuals, unless otherwise approved by the Contracting Officer. The procedures must be approved by the EPA prior to use. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval, by the Contracting Officer in consultation with authorized EPA officials at EPA's discretion. The Contractor shall not proceed with notification unless the Contracting Officer has determined in writing that notification is appropriate.

(c) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(1) A brief description of the incident;
(2) A description of the types of PII and Sensitive PII involved;
(3) A statement as to whether the PII or Sensitive PII was encrypted or protected by other means;
(4) Steps individuals may take to protect themselves;
(5) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(6) Information identifying who individuals may contact for additional information, including contractor name and point of contact (POC) and contract number.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task O - Credit Monitoring and Identity Protection

(a) Definitions.

(1) *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(2) *Personally Identifiable Information (PII)*, as defined in OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to sensitive information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment made by the EPA Privacy Officer of the specific risk that an individual can be identified. Non-PII

can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

(3) *Sensitive PII* refers to personally identifiable information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling than PII because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

(b) *Credit Monitoring Requirements*. In the event that an Information Security Incident involves PII or Sensitive PII, the Contractor may be required to do the following tasks as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described in the "Individual Notification for Personally Identifiable Information" requirement;

(2) Provide credit monitoring and identity protection services to individuals whose data was under the control of the Contractor or resided in the Contractor information technology (IT) system at the time of the Information Security Incident for a period beginning the date of the Incident and extending not less than 18 months from the date the individual is notified; and/or

(3) Use a dedicated call center; or establish one if necessary and as authorized in writing by the Contracting Officer. Call center services provided by the Contractor shall include:

(i) A dedicated telephone number for affected individuals to contact customer service within a fixed time period as determined by the Contracting Officer;

(ii) Information necessary for affected individuals to access credit reports and credit scores;

(iii) Weekly reports submitted to the Task Order Contracting Officer's Representative (TOCOR) on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or EPA, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or EPA for resolution, as appropriate;

(v) Preparation of customized frequently-asked-questions-and-answers (FAQs), in consultation as applicable with other parties like subject matter experts and TOCORs, and that must be approved in advance in writing by the Contracting Officer; and

(vi) Information for affected individuals to contact customer service representatives and fraud resolution representatives for credit monitoring and identity protection assistance.

(c) *Credit monitoring and identity protection services.* At a minimum, the Contractor shall provide the following credit monitoring and identity protection services:

(1) Triple credit bureau monitoring with Equifax, Experian and Transunion;

(2) Daily customer service;

(3) Alerts provided to the individual for changes in credit posture and fraud; and/or

(4) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task P - Compliance with IT Security Policies

(a) Information systems and system services provided to EPA by the Contractor must comply with current EPA information technology (IT), IT security, physical and personnel security and privacy policies and guidance, and EPA Acquisition Regulation 1552.211-79, *Compliance with EPA Policies for Information Resources Management*.

(b) Contractors are also required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA) of 2014, Privacy Act of 1974, E-Government Act of 2002, Federal Information Processing Standards (FIPS), the 500- and SP500- and 800-Series Special Publications (SP), Office of Management and Budget (OMB) memoranda and other relevant Federal laws and regulations that are applicable to EPA.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task Q - Secure Technical Implementation

(a) The Contractor shall use applications that are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB).

(b) The Contractor's standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration.

(c) Contractor applications designed for normal/regular, i.e., non-privileged end users must run in the standard user context without elevated system administration privileges.

(d) The Contractor shall apply due diligence always to ensure that Federal Information Processing Standard (FIPS) 199 “moderate confidentiality impact” security is always in place to protect EPA systems and information.

(e) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task R - Internet Protocol Version 6 (IPv6)

(a) In accordance with EPA technical standards, all system hardware, software, firmware, and/or networked component or service (voice, video, or data) utilized, developed, procured, acquired or delivered in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and/or storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, devices and systems shall maintain interoperability with IPv4 products.

(b) Any IP product or system utilized, developed, acquired, produced or delivered must interoperate with both IPv6 and IPv4 systems and products, in an equivalent or better way than current IPv4 capabilities with regard to functionality, performance, management and security; and have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(c) As IPv6 evolves, the Contractor shall upgrade or provide an appropriate migration path for each item developed, delivered or utilized, at no additional cost to the Government. The Contractor shall retrofit all non-IPv6 capable equipment, as defined above, which is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.

(d) The Contractor shall provide technical support for both IPv4 and IPv6.

(e) All Contractor-provided system or software must be able to operate on networks supporting IPv4, IPv6, or one supporting both.

(f) Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance, at no additional cost to the Government.

(g) EPA reserves the right to require the Contractor’s products to be tested within an EPA or third-party test facility to demonstrate contract compliance.

(h) In accordance with FAR 11.002(g), this acquisition must comply with the National Institute

of Standards and Technology (NIST) US Government (USG) v6 Profile and IPv6 Test Program. The Contractor shall fund and provide resources necessary to support these testing requirements, and it will not be paid for as a direct cost under the subject contract.

(i) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task S - Cloud Service Computing

(a) The Contractor handling EPA information or operating information systems on behalf of EPA must protect EPA information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction per the Federal Information Security Modernization Act (FISMA) and EPA policy.

(b) EPA information stored in a cloud environment remains the property of EPA, and not the Contractor or cloud service provider (CSP). The Contractor may also be the CSP. EPA retains ownership of the information and any media type that stores Government information.

(c) In the event the Contractor is the CSP or can control the CSP through a subcontracting or other business relationship then the following requirements will apply:

(1) The CSP does not have rights to use the EPA information for any purposes other than those explicitly stated in the contract or applicable "Rights in Data" contract requirements.

(2) The CSP must protect EPA information from all unauthorized access.

(3) The CSP must allow EPA access to EPA information including data schemas, metadata, and other associated data artifacts that are required to ensure EPA can fully and appropriately retrieve EPA information from the cloud environment that can be stored, read, and processed.

(4) The CSP must have been evaluated by a Third Party Assessment Organization (3PAO) certified under the Federal Risk and Authorization Management Program (FedRAMP). The Contractor must provide the most current, and any subsequent, Security Assessment Reports to the Task Order Contracting Officer's Representative (TOCOR) for consideration by the Information Security Officer (ISO) as part of the Contractor's overall Systems Security Plan.

(5) The Contractor must require the CSP to follow cloud computing contract best practices identified in "Creating Effective Cloud Computing Contracts for the Federal Government" produced by the Federal Chief Information Officer (CIO) Council and Federal Chief Acquisition Officers Council.

(d) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task T - Contract Performance Information and Testimony

(a) Dissemination of Contract Performance Information. The Contractor must not publish, permit to be published, or distribute to the public, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. A copy of any material proposed to be published or distributed must be submitted to the Contracting Officer for written approval prior to publication.

(b) Contractor Testimony. All requests for the testimony of the Contractor or its employees, and any intention to testify as an expert witness relating to: (a) any work required by, and or performed under, this contract; or (b) any information provided by any party to assist the Contractor in the performance of this contract, must be immediately reported to the Contracting Officer.

(c) *Subcontract flowdown*. The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.

Task U - Rehabilitation Act Section 508 Standards/IT Accessibility Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

1. Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines

Applicable Functional Performance Criteria: All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

Applicable requirements for software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable requirements for hardware features and components: All requirements apply

Instructions

1. Provide an Accessibility Conformance Report (ACR) for each commercially available Information and Communication Technology (ICT) item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version

2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. Provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. Describe your approach to incorporating universal design principles to ensure ICT products or services are designed to support disabled users.

3. Describe plans for features that do not fully conform to the Section 508 Standards.

4. Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the ICT product or service being offered.

Prior to acceptance, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

Task V - Termination for Default - Failure to Report Information Security Incident

(a) Definition. *Information Security Incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(b) If the Contractor was aware of an Information Security Incident and did not disclose it in accordance with the requirements specified in this contract or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

(c) The Contractor agrees to insert in each subcontract or consultant agreement placed hereunder, provisions which shall conform substantially to the language of this requirement, including this paragraph, unless otherwise authorized by the Contracting Officer.